



OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
HEALTH AFFAIRS
SKYLINE FIVE, SUITE 810, 5111 LEESBURG PIKE
FALLS CHURCH, VIRGINIA 22041-3206

TRICARE
MANAGEMENT
ACTIVITY

SEP 9 2004

MEMORANDUM FOR DEPUTY SURGEON GENERAL OF THE ARMY
DEPUTY SURGEON GENERAL OF THE NAVY
DEPUTY SURGEON GENERAL OF THE AIR FORCE

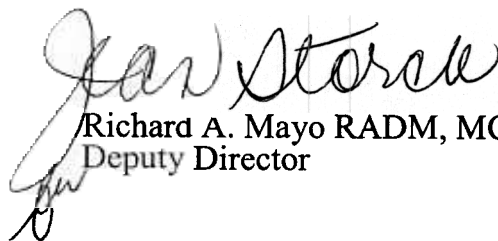
SUBJECT: Request to Appoint Medical Treatment Facility and Dental Treatment Facility
Health Insurance Portability and Accountability Act of 1996 Security Officials

The Health Insurance Portability and Accountability Act (HIPAA) of 1996, Public Law 104-191, administrative simplification provisions require the protection and privacy of individually identifiable health information. The HIPAA Security rule, signed in February 2003, mandates the standards for the integrity, confidentiality, and availability of electronically protected health information. Full compliance with its requirements must be met by April 21, 2005.

The purpose of this memorandum is to request the appointment of a HIPAA Security Official at each military treatment facility and dental treatment facility (MTF/DTF). HIPAA Security Officials will be responsible for managing the development and implementation of security policies, standards, guidelines, and procedures to ensure ongoing maintenance of the security of health information and compliance with the HIPAA Security Rule. Responsibilities also include managing and supervising the conduct of personnel in relation to those measures. Based on the size and complexity of the MTF/DTF, a HIPAA Security Official may be responsible for more than one facility in a geographic area when smaller facilities can share resources under a mutually acceptable agreement. The HIPAA Security Official will be the MTF/DTF point of contact for HIPAA Security implementation and receive training and guidance from the respective Service HIPAA Program Office. Suggested roles and responsibilities are described in the attachment to this memorandum. It is imperative that the person selected as the MTF/DTF HIPAA Security Official has the requisite experience, knowledge and authority to develop, implement and monitor the security practices, policies and procedures throughout the facility.

Please forward the name, phone number and e-mail address of the appointed MTF/DTF HIPAA Security Official to your respective Service Headquarters HIPAA Security Integrated Project Team representative and to the TRICARE Management Activity Privacy Office.

Questions regarding this request may be directed to Mr. Sam Jenkins, TMA Privacy Officer, 5111 Leesburg Pike, Suite 810, Falls Church, Virginia, 22041, or by email: Sam.Jenkins@tma.osd.mil, or fax: 703-681-8845.

A handwritten signature in black ink, appearing to read "Richard A. Mayo".

Richard A. Mayo RADM, MC, USN
Deputy Director

Attachment:
As stated

cc:
Dr. Richard Guerin
Mr. Sam Jenkins

**HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT
MEDICAL TREATMENT FACILITY/DENTAL TREATMENT FACILITY
SECURITY OFFICIAL
ROLES AND RESPONSIBILITIES**

Organizational Need/Function: The Security Rule of the Health Insurance Portability and Accountability Act (HIPAA) of 1996, Public Law 104-191, requires Medical Treatment Facility and Dental Treatment Facility (MTF/DTF) personnel to be assigned the responsibility of managing and supervising the execution and use of security measures to protect data as well as the responsibility of managing and supervising the conduct of personnel in relation to those measures.

ROLES AND RESPONSIBILITIES

Policy Implementation, Oversight, Auditing and Compliance:

- Manage the development and implementation of security policies, standards, guidelines, and procedures to ensure ongoing maintenance of the security of health information and compliance with the HIPAA Security Rule.
- Identify and review the security features of existing and new computing systems to ensure that they meet the security requirements of existing policies. Review and propose changes to existing policies and procedures that reflect the existing requirements of the systems to which they apply. Periodically reassess status and updated security standards established by the facility.
- Monitor day-to-day entity operations and systems for compliance. Report to management on the status of compliance.
- Periodically assess current security compliance status vs. necessary status (gap analysis).
- Work with management, the medical staff, the director of health information management, the Privacy Officer, and others to ensure protection of patient privacy and confidentiality in a manner that does not compromise the entity, its personnel, good medical practice, or proper health information management practices.
- Develop and/or ensure internal controls are capable of preventing and detecting significant instances or patterns of illegal, unethical, or improper conduct.
- Coordinate or oversee the filing of regulatory forms, reports, etc. Assist other departments in understanding and complying with regulatory requirements. Work with appropriate individuals to ensure facility implements and maintains appropriate security forms, materials, processes, procedures, and practices.
- Respond to alleged violations of rules, regulations, policies, procedures, and codes of conduct by evaluating or recommending the initiation of investigative procedures.
- Ensures consistent action is taken for failure to comply with security policies for all employees in the workforce. Works in cooperation with human resources, administration, and legal counsel, as appropriate.

- ◆ Identify potential areas of compliance vulnerability and risk; develop/implement corrective action plans for the resolution of problematic issues and provide guidance on how to avoid or deal with similar situations.
- ◆ Establish and chair the interdisciplinary Medical Information Security Readiness Team. Ensure that the team includes at least one clinical, one patient administration, and one information technology representative. The team is responsible for coordinating MTF/DTF implementation of HIPAA Security and protecting the confidentiality, integrity and availability of electronic protected health information.
- ◆ Perform internal audit of data access and use to detect and deter breaches.
- ◆ Receive reports of Security breaches, take appropriate action to minimize harm, investigate breaches, and make recommendations to management for corrective action.

Education, Training and Communication:

- Provide the facility's information security policies and practices to employees and others with access to health information. Prepare and publish papers/articles on good security practices for the facility's employees and others. Ensure that training conforms to existing policies and procedures.
- Communicate the importance of compliance and the compliance program to senior management, the compliance committee, and health plan staff.
- Work with leadership to provide adequate information to ensure that they and their employees have the requisite information and knowledge of regulatory issues and requirements to carry out their responsibilities in a lawful and ethical manner.
- Provide input and/or direction to the employee performance appraisal and incentive programs to ensure improper conduct is reported and discouraged and that support of and conformity with the compliance program is part of any performance evaluation process for all employees.

MTF Integration Activities:

- In coordination with key personnel, develop and implement the following plans and others as required:
 - Disaster plan, emergency mode operation plan, backup plan, physical security plan, personnel security plan, access policies, and others. Test and revise plans as necessary to ensure data integrity, confidentiality, and availability.
- Function as key representative/liaison in meetings regarding regulatory policy.